

Cursor flaw gives Vista security a black eye

By Joris Evers

http://news.com.com/Cursor+flaw+gives+Vista+security+a+black+eye/2100-1002_3-6173115.html

Story last modified Wed Apr 04 15:22:45 PDT 2007

Microsoft's release of a "critical" patch on Tuesday poked holes in Vista's security promises, but security experts advise against discounting the new operating system.

The software giant [broke with its monthly patch cycle Tuesday](#) to fix a bug that cybercrooks had been [using since last week to attack Windows PCs](#), including those running Vista.

"As far as software vulnerabilities go, Vista's cover is blown," said Nand Mulchandani, a vice president at Determina, the company that discovered the latest security bug. "It is not Superman; it is just a human being. It is just software. Vista is going to be very similar to the other operating systems Microsoft has delivered in terms of bugs."

Microsoft officially [launched Vista for consumers in January](#), promoting the operating system as the [most secure version of Windows yet](#). It is the first client version of Windows built with security in mind, meaning that it should have fewer coding errors that might be exploited in attacks, Microsoft has said.

Yet the "critical" hole that affected much older Windows versions [also hit Vista](#). The vulnerability lies in the way Windows handles animated cursors and could let an attacker commandeer a PC when the user views a malicious Web site or e-mail message.

The cursor flaw lies in the operating system code. This means that any application that relies on the operating system to handle animated cursor files could be an attack vector. This includes alternative browsers, such as Firefox.

It is a flaw that should have been caught by Microsoft's code-vetting processes for [Vista](#), called the Security Development Lifecycle, some experts said. The flaw is also evidence that faulty code from previous Windows versions has been copied into Vista, they said.



"It is a little premature to attack the whole effort altogether, but this is something that the Security Development Lifecycle should have caught," said Amol Sarwate, a research manager at vulnerability management company Qualys.

Video: [Hacking a Vista PC](#)

Determina experts explain how to exploit animated-cursor flaw.

The buffer overflow vulnerability in the cursor function in particular should have already been fixed because a bug in the same Windows component was patched two years ago, said Rohit Dhamankar, manager of security research at TippingPoint, a seller of intrusion prevention products. That should have prompted re-examination of the code, Dhamankar said.

Microsoft disputes that it should have caught the cursor bug before. People who say so don't understand security vulnerabilities because not all bugs are created equal, said Stephen Toulouse, senior product manager in Microsoft's Security Technology Unit.

"In the case of the cursor vulnerability, even though something may look similar to the outside, that doesn't mean the code is anything alike to the previous vulnerability," Toulouse said. "The SDL was never meant to catch every single vulnerability, period."

But Dhamankar argues that Microsoft forgot to recheck all the possibilities that could lead to a buffer overflow after the original bug was found and patched in 2005.

Mulchandani agreed. "The dirty little secret is that Microsoft clearly did not write Vista from scratch. They did not completely build a whole new code base for this operating system. Every version of Windows since Windows NT has had this flaw in it," he said.

Microsoft does acknowledge that Vista will have vulnerabilities. "There are going to be other vulnerabilities. The SDL is not a process by which no vulnerabilities will ever occur. There is no process on this planet that can do that," Toulouse said.

The cursor flaw is like [a sign post for the bug hunters](#). Hackers will now be looking for bugs in similar Windows components to find ways to attack Vista.

Now on News.com:

"This has been a very significant break and it definitely gives a big pointer," Dhamankar said. "If more such errors are found later, Vista is not going to be able to offer the great protection that's claimed."

Still, Microsoft's Vista security promise doesn't fall apart because of this single vulnerability. Vista is more secure than XP or any other Microsoft client operating system, Sarwate said. "If you consider Windows 2000, XP, 2003, I would still say that Vista is more secure than all the other operating systems," he said.

Mulchandani also said that, while Microsoft has taken way too big a bite at the security message, Vista is more secure than its predecessors because of features [such as User Account Control](#) and others that limit privileges on the operating system.

And that's just the goal Microsoft was aiming for, Toulouse said.

"You have to look at Vista versus XP. A lot of people are holding Vista up and saying in a vacuum it will reach some nirvana of security," Toulouse said. "Our whole goal with Windows Vista was to create a fundamentally more secure operating system than we have ever created previously."

[Copyright](#) ©1995-2007 CNET Networks, Inc. All rights reserved.

- [IBM adds low-wattage x86 servers](#)
- [Tech tips for parents of Web-surfing kids](#)
- [Rewriting ethics rules for the new media](#)
- [Extra: The 21 biggest technology flops](#)
- [Video: Mashups for all](#)